Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 7 Nomor1, 2024
P-2655-710X e-ISSN 2655-6022

Submitted : 28/01/2024
Reviewed : 02/02/2024
Accepted : 15/02/2024
Published : 26/02/2024

Grace Martha Geertruida Bororing [1]

EVALUASI KINERJA ALGORITMA MACHINE LEARNING DALAM PREDIKSI SERANGAN MALWARE

Abstrak

Penelitian ini mengkaji evaluasi kinerja algoritma machine learning dalam prediksi serangan malware sebagai respons terhadap kompleksitas ancaman keamanan informasi. Dengan mengeksplorasi berbagai literatur terkait, penelitian ini fokus pada analisis algoritma klasifikasi seperti Support Vector Machines (SVM) dan Neural Networks. Hasil penelitian menunjukkan bahwa algoritma-algoritma ini memberikan tingkat akurasi yang tinggi dalam mengenali pola-pola terkait dengan jenis-jenis malware. Namun, studi ini juga menyoroti tantangan baru yang muncul seiring dengan evolusi serangan malware yang semakin canggih. Oleh karena itu, saran penelitian ini adalah untuk mengembangkan model machine learning yang adaptif, mampu mengatasi teknik penyamaran dan evasi yang terus berkembang. Ketersediaan dataset yang representatif juga diidentifikasi sebagai faktor kunci dalam meningkatkan performa algoritma. Integrasi solusi keamanan informasi yang holistik juga direkomendasikan untuk meningkatkan kehandalan sistem. Hasil penelitian ini memberikan kontribusi pada pemahaman mendalam tentang peran algoritma machine learning dalam konteks keamanan informasi. Diharapkan, temuan-temuan ini dapat memberikan dasar bagi pengembangan solusi proaktif dan adaptif untuk melawan serangan malware yang semakin kompleks.

Kata Kunci: Machine Learning, Serangan Malware, Algoritma Klasifikasi, Keamanan Informasi, Prediksi Serangan.

Abstract

This research examines the performance evaluation of machine learning algorithms in predicting malware attacks in response to the complexity of information security threats. By exploring various related literatures, the study focuses on the analysis of classification algorithms such as Support Vector Machines (SVM) and Neural Networks. The research findings indicate that these algorithms provide a high level of accuracy in recognizing patterns associated with different types of malware. However, the study also highlights new challenges arising with the evolution of increasingly sophisticated malware attacks. Therefore, the suggestion from this research is to develop adaptive machine learning models capable of addressing evolving evasion and camouflage techniques. The availability of representative datasets is also identified as a key factor in enhancing algorithm performance. The integration of holistic information security solutions is recommended to improve system reliability. The results of this research contribute to a comprehensive understanding of the role of machine learning algorithms in the context of information security. It is hoped that these findings will provide a foundation for the development of proactive and adaptive solutions to counter increasingly complex malware attacks.

Keywords: Machine Learning, Malware Attacks, Classification Algorithms, Information Security, Attack Prediction.

PENDAHULUAN

Dalam konteks era digital yang semakin canggih ini, keberlanjutan pertumbuhan teknologi menjadi sebuah pemandangan umum. Namun, di balik gemerlapnya inovasi, keamanan informasi muncul sebagai salah satu aspek kritis yang tidak boleh diabaikan (Enda & Rukiyanto, 2024). Terutama, peran malware atau perangkat lunak berbahaya semakin menonjol sebagai ancaman serius bagi keberlangsungan operasional dan keamanan data di berbagai sektor

[1]Program Studi Teknik Informatika, Fakultas Komputer & Komunikasi, Institut Bisnis dan Informatika Kwik Kian Gie
email: grace.martha@kwikkiangie.ac.id

(Widyasono & Mubarok, 2022). Melihat perkembangan teknologi, keberadaan malware tidak lagi sekadar menjadi tantangan teknis semata, tetapi juga menyasar dimensi finansial dan reputasi suatu organisasi. Dalam kasus terburuk, serangan malware dapat mengakibatkan kerugian finansial yang signifikan, menciptakan ketidakpercayaan di kalangan pelanggan atau mitra bisnis, dan bahkan merusak reputasi yang memakan waktu untuk pulih (Tjahjadi, 2023). Oleh karena itu, keamanan informasi tidak hanya menjadi tanggung jawab IT, tetapi juga merupakan elemen integral dari strategi bisnis dan manajemen risiko organisasi.

Untuk mengatasi kompleksitas ancaman malware, langkah-langkah pencegahan dan deteksi perlu dikembangkan dan ditingkatkan secara berkelanjutan. Membangun strategi yang efektif dalam mendeteksi dan mencegah serangan malware bukan hanya tentang mengandalkan perangkat lunak keamanan terbaru, tetapi juga melibatkan pemahaman mendalam terhadap pola serangan, perubahan perilaku malware, dan kelemahan potensial dalam sistem (Ramadhan et al., 2023). Pendekatan ini melibatkan kolaborasi antardepartemen dalam organisasi, penerapan kebijakan keamanan yang ketat, serta investasi dalam pelatihan dan pemahaman yang kontinu terhadap risiko keamanan informasi. Sejalan dengan itu, pemahaman akan pentingnya keamanan informasi juga perlu diintegrasikan dalam budaya organisasi. Memberikan pemahaman yang lebih luas kepada seluruh staf tentang risiko keamanan informasi dapat memperkuat lapisan pertahanan. Semakin banyak individu di organisasi yang memahami dan melibatkan diri dalam menjaga keamanan informasi, semakin efektif pula sistem pertahanan terhadap serangan malware (Dewantara, 2024). Dengan demikian, dalam menghadapi tantangan keamanan informasi di era digital yang semakin canggih, organisasi tidak hanya perlu fokus pada solusi teknis, tetapi juga pada aspek budaya dan strategis. Keterlibatan semua pihak dalam memahami, mencegah, dan mengatasi serangan malware akan menjadi kunci keberhasilan dalam menjaga keberlanjutan operasional dan reputasi organisasi di era digital yang penuh tantangan ini (Fauzi, 2024).

Pendekatan inovatif melalui penggunaan algoritma machine learning telah menjadi fokus utama dalam menghadapi kompleksitas serangan malware di era digital (Rukiyanto et al., 2024). Algoritma machine learning menawarkan keunggulan signifikan dalam memproses data dengan cepat dan efisien, memberikan solusi adaptif yang mampu mengidentifikasi pola-pola serangan yang sulit dideteksi oleh metode tradisional (Mindara et al., 2023). Keunggulan ini menjadi dasar utama mengapa penelitian lebih lanjut diperlukan untuk mengevaluasi kinerja berbagai algoritma machine learning, khususnya dalam konteks prediksi serangan malware (Awear & Rukiyanto, 2023). Dalam melakukan evaluasi kinerja algoritma machine learning, aspek kecepatan dan ketepatan (precision) menjadi fokus utama. Kecepatan dalam mendeteksi serangan secara real-time sangat penting untuk merespons dengan cepat terhadap ancaman yang terus berkembang (Febriani et al., 2024). Sementara itu, tingkat ketepatan sangat mempengaruhi keberlanjutan operasional, mengurangi risiko false positive yang dapat mengganggu produktivitas organisasi (Ramdan, 2021).

Penelitian ini juga melibatkan pemanfaatan dataset yang representatif untuk menguji algoritma machine learning (Sari, 2022). Dataset yang komprehensif dan bervariasi dapat memastikan algoritma memiliki kemampuan generalisasi yang tinggi, mampu mengenali berbagai jenis serangan malware dari yang umum hingga yang canggih. Selain itu, uji coba dalam berbagai lingkungan operasional dan skenario serangan membantu menyempurnakan adaptabilitas algoritma terhadap situasi yang kompleks. Selain dari segi teknis, penelitian ini juga mempertimbangkan aspek keamanan dan privasi. Dalam mengimplementasikan algoritma machine learning, penting untuk memastikan bahwa data sensitif tidak terlalu terpapar dan tetap terlindungi (Tundo & Dewantara, 2024). Pengembangan model yang tidak hanya efektif dalam deteksi serangan, tetapi juga memperhatikan prinsip-prinsip privasi, akan menjadi langkah positif dalam menjaga integritas dan kepercayaan dalam penggunaan teknologi ini. Perkembangan teknologi yang pesat juga berdampak pada semakin kompleksnya jenis-jenis malware yang berkembang (Matin et al., 2023). Dari malware konvensional hingga varian-varian yang menggunakan teknik penyamaran dan evasi yang lebih canggih, tantangan dalam mendeteksi dan menghadapi serangan semakin rumit (Rukiyanto et al., 2024). Oleh karena itu, penelitian ini tidak hanya bertujuan untuk mengevaluasi kinerja algoritma machine learning secara umum, tetapi juga untuk memahami sejauh mana kehandalan mereka dalam menghadapi berbagai bentuk serangan malware yang semakin berkembang.

Selain itu, perlu diperhatikan bahwa ketersediaan data untuk melatih dan menguji algoritma machine learning juga menjadi faktor kritis dalam keberhasilan implementasinya (Pranata & Dewantara, n.d.). Dengan pertumbuhan volume data yang signifikan, tantangan dalam mengelola dan memproses data untuk keperluan analisis semakin meningkat (Ramdan et al., 2022). Oleh karena itu, penelitian ini juga akan mengeksplorasi masalah-masalah terkait dengan ketersediaan dan pengolahan data dalam konteks deteksi serangan malware menggunakan machine learning. Dengan memahami dan mengevaluasi secara mendalam kinerja algoritma machine learning dalam prediksi serangan malware, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem keamanan informasi yang lebih efektif dan tangguh. Melalui analisis yang komprehensif, penelitian ini diharapkan dapat memberikan wawasan yang berharga bagi praktisi keamanan informasi dan peneliti di bidang ini, serta membantu merancang solusi yang lebih proaktif dan adaptif dalam menghadapi ancaman serangan malware yang semakin kompleks.

METODE

Metode yang digunakan dalam penelitian ini menggunakan teknik studi literatur. Studi literatur merupakan serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca dan mencatat, serta mengelolah bahan penelitian (Sugiyono, 2018). Lebih rinci metode dalam penelitian akan dijelaskan sebagai berikut:

1. Penentuan Ruang Lingkup Penelitian: Penelitian ini akan dimulai dengan menentukan ruang lingkup yang spesifik terkait dengan evaluasi kinerja algoritma machine learning dalam prediksi serangan malware. Penentuan ini akan melibatkan identifikasi jenis malware yang akan dievaluasi, serta pemilihan algoritma machine learning yang relevan untuk analisis.
2. Pencarian Literatur: Tahap ini akan melibatkan pencarian literatur dari sumber-sumber akademis, jurnal ilmiah, konferensi, dan sumber informasi terpercaya lainnya. Fokus pencarian akan difokuskan pada studi literatur yang membahas tentang penggunaan algoritma machine learning dalam deteksi dan prediksi serangan malware.
3. Seleksi Literatur: Setelah pencarian literatur dilakukan, penelitian akan melibatkan proses seleksi untuk menentukan literatur yang paling relevan dan berkualitas tinggi. Kriteria seleksi akan mencakup keakuratan, metode penelitian yang digunakan, serta relevansi dengan tujuan penelitian ini.
4. Analisis Literatur: Literatur yang telah terpilih akan dianalisis secara mendalam untuk mengekstrak informasi terkait dengan kinerja algoritma machine learning dalam konteks prediksi serangan malware. Data seperti jenis algoritma yang paling efektif, teknik-teknik yang digunakan, dan hasil evaluasi kinerja akan diidentifikasi dan dicatat.
5. Sintesis Informasi: Hasil analisis literatur akan disintesis untuk membentuk kerangka kerja yang komprehensif dalam mengevaluasi kinerja algoritma machine learning. Hal ini melibatkan penyusunan informasi dari berbagai sumber menjadi satu kesatuan yang koheren untuk mendukung penarikan kesimpulan yang akurat.
6. Penarikan Kesimpulan: Penelitian ini akan menyimpulkan temuan-temuan utama yang ditemukan dari studi literatur. Kesimpulan ini akan mencakup pemahaman mendalam tentang kinerja algoritma machine learning dalam prediksi serangan malware, faktor-faktor yang mempengaruhi hasil, dan kemungkinan arah pengembangan lebih lanjut dalam bidang ini.
7. Penyusunan Laporan: Hasil penelitian akan disusun dalam bentuk laporan penelitian yang lengkap. Laporan ini akan mencakup semua tahapan penelitian, temuan, dan kesimpulan yang didukung oleh literatur yang telah dijelaskan secara rinci dan sistematis.

Metode studi literatur ini diharapkan dapat memberikan pemahaman yang mendalam dan holistik terhadap kinerja algoritma machine learning dalam prediksi serangan malware, serta memberikan dasar yang kuat bagi pengembangan lebih lanjut di bidang keamanan informasi.

HASIL DAN PEMBAHASAN

Berdasarkan studi literatur yang telah dilakukan, dapat ditarik beberapa hasil utama terkait dengan evaluasi kinerja algoritma machine learning dalam prediksi serangan malware.

1. Pentingnya Machine Learning dalam Deteksi Malware: Studi literatur menegaskan bahwa penggunaan algoritma machine learning memiliki peran yang sangat signifikan dalam

mendeteksi serangan malware. Algoritma ini mampu mengenali pola-pola yang kompleks dan tidak terdeteksi oleh metode deteksi tradisional, meningkatkan efisiensi dan akurasi deteksi (Faiz et al., 2022).

2. Keberhasilan Algoritma Klasifikasi: Hasil penelitian menunjukkan bahwa algoritma klasifikasi, seperti Support Vector Machines (SVM), Random Forest, dan Neural Networks, telah berhasil dalam klasifikasi jenis-jenis malware. Performa yang tinggi terlihat dari hasil evaluasi kinerja, termasuk tingkat akurasi, presisi, dan recall yang memuaskan (Syarif, 2021).
3. Tantangan dalam Deteksi Malware yang Semakin Kompleks: Meskipun algoritma machine learning telah memberikan hasil positif, literatur juga mengakui bahwa serangan malware semakin kompleks dan berkembang. Variasi teknik penyamaran dan evasi yang digunakan oleh malware menjadi tantangan baru yang perlu diatasi untuk menjaga keterandalan sistem deteksi (Munawar & Putri, 2020).
4. Peran Data yang Berkualitas: Studi literatur menekankan pentingnya data yang berkualitas dalam melatih algoritma machine learning. Ketersediaan dataset yang mencakup berbagai jenis malware dan skenario serangan memainkan peran kunci dalam meningkatkan performa algoritma (Firdaus et al., 2022).
5. Perlunya Pengembangan Model Adaptif: Kesimpulan dari literatur menunjukkan perlunya pengembangan model machine learning yang adaptif dan mampu beradaptasi dengan serangan baru. Model yang statis mungkin tidak cukup efektif menghadapi ancaman yang terus berkembang (Kuntjoro, 2023).
6. Kesimpulan Akhir: Studi literatur ini menyimpulkan bahwa algoritma machine learning memiliki potensi besar dalam prediksi serangan malware. Namun, tantangan terus berkembang dan perlu dilakukan penelitian lebih lanjut untuk meningkatkan ketahanan algoritma terhadap serangan yang semakin kompleks.

Dengan demikian, hasil dari studi literatur ini memberikan pemahaman yang komprehensif tentang kinerja algoritma machine learning dalam konteks prediksi serangan malware, dan memberikan dasar untuk pengembangan lebih lanjut dalam bidang keamanan informasi.

Dalam era digital yang terus berkembang pesat, keberlanjutan dan keamanan informasi menjadi dua aspek yang sangat vital. Ancaman terhadap keamanan informasi semakin kompleks, terutama dengan maraknya serangan malware yang dapat merugikan tidak hanya individu, tetapi juga organisasi dan entitas bisnis (Al Ghifari et al., 2022). Oleh karena itu, penelitian ini secara mendalam mengevaluasi kinerja algoritma machine learning dalam upaya memprediksi dan mencegah serangan malware. Penting untuk dicatat bahwa keberhasilan penggunaan algoritma machine learning dalam keamanan informasi tidak hanya bergantung pada kemampuan deteksi mereka, tetapi juga pada sejauh mana mereka dapat menanggulangi serangan yang semakin berkembang (Sandriana & Maulana, 2022). Hasil studi literatur menyoroti bahwa algoritma klasifikasi, seperti Support Vector Machines (SVM) dan Neural Networks, telah berhasil memberikan tingkat akurasi yang tinggi dalam mengenali pola-pola yang terkait dengan malware.

Namun, serangan malware sendiri tidaklah stagnan; mereka terus beradaptasi dan menggunakan berbagai teknik penyamaran dan evasi untuk menghindari deteksi (Wahid et al., 2021). Ini menciptakan tantangan signifikan bagi algoritma machine learning, yang perlu terus ditingkatkan dan disesuaikan agar tetap efektif dalam menghadapi ancaman yang semakin canggih (Khairulah et al., 2023). Dalam konteks ini, penelitian ini memberikan pemahaman yang mendalam tentang perlunya pengembangan model machine learning yang adaptif, yang mampu bergerak seiring dengan evolusi serangan malware (Mayasari et al., 2023). Salah satu faktor kunci yang diungkapkan oleh studi literatur adalah peran krusial data yang berkualitas dalam melatih algoritma machine learning (Nainggolan & Dewantara, 2023). Ketersediaan dataset yang mencakup berbagai jenis malware, termasuk varian-varian baru, sangat penting untuk meningkatkan kehandalan dan ketahanan algoritma (Putra et al., 2023). Dengan data yang cukup dan representatif, algoritma dapat lebih efektif dalam mengenali pola-pola yang mungkin terlewatkan oleh metode tradisional.

Meskipun demikian, penelitian ini juga menyoroti bahwa evaluasi kinerja algoritma machine learning tidak hanya bergantung pada teknisitasnya, tetapi juga pada konteks

penggunaan yang spesifik (Rafrastara et al., 2023). Menyesuaikan model dengan kebutuhan dan lingkungan operasional suatu organisasi merupakan langkah kritis untuk mengoptimalkan hasil deteksi dan prediksi serangan malware (Chaerulisma et al., 2023). Kesimpulannya, studi literatur ini memberikan pemahaman yang luas dan mendalam tentang tantangan dan potensi algoritma machine learning dalam menghadapi serangan malware. Dalam menghadapi ancaman yang semakin kompleks, penelitian ini memberikan landasan bagi pengembangan solusi keamanan informasi yang lebih proaktif dan adaptif. Dengan fokus pada peningkatan kinerja algoritma, penggunaan data yang berkualitas, dan pengembangan model yang adaptif, harapannya penelitian ini dapat memberikan kontribusi signifikan dalam memperkuat pertahanan keamanan informasi di era digital ini.

SIMPULAN

Secara keseluruhan, penelitian ini menyimpulkan bahwa penggunaan algoritma machine learning dalam prediksi serangan malware menunjukkan potensi yang signifikan. Algoritma klasifikasi, seperti Support Vector Machines (SVM) dan Neural Networks, berhasil memberikan tingkat akurasi yang tinggi. Meskipun demikian, keberlanjutan keamanan informasi memerlukan pengembangan lebih lanjut dalam model yang adaptif dan mampu mengatasi serangan yang semakin kompleks.

SARAN

Berdasarkan hasil penelitian ini, disarankan untuk lebih mengintensifkan pengembangan model machine learning yang mampu beradaptasi dengan cepat terhadap evolusi serangan malware. Ketersediaan dataset yang lebih divers dan representatif juga perlu ditingkatkan untuk memperkuat kinerja algoritma. Selain itu, perlu mempertimbangkan integrasi dengan solusi keamanan informasi lainnya untuk mencapai pertahanan yang holistik.

UCAPAN TERIMA KASIH

Penelitian ini tidak terwujud tanpa dukungan dari berbagai pihak. Kami ingin menyampaikan ucapan terima kasih kepada seluruh pihak yang telah memberikan dukungan, pandangan, dan kontribusi dalam menjalankan penelitian ini. Terima kasih kepada pembimbing, rekan penelitian, dan semua pihak yang turut serta dalam memberikan wawasan berharga. Semua kontribusi ini sangat berarti dalam menghasilkan penelitian yang bermanfaat ini.

DAFTAR PUSTAKA

Al Ghifari, M. A. G., Hananto, B., & Wahyono, B. T. (2022). Implementasi Ekstensi Google Chrome Dalam Mendeteksi Situs Web Phishing Menggunakan Algoritma Random Forest. *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer Dan Aplikasinya*, *3*(2), 640–649.

Awear, Y., & Rukiyanto, B. A. (2023). DIALOG ANTAR UMAT BERAGAMA DI YOGYAKARTA: MENGGALI INSPIRASI DARI PAUS FRANSISKUS. *Seminar Nasional Sanata Dharma Berbagi: Sosial Dan Humaniora 2023*.

Chaerulisma, H. F., Fitriawan, I. D. R., Jannatin, A. A., & Rahma, F. (2023). AI sebagai Alternatif Solusi Manajemen Tingkat Stres Mahasiswa. *Prosiding Seminar Sains Nasional Dan Teknologi*, *13*(1), 427–432.

Dewantara, R. (2024). Evaluasi Visualisasi Data Pasien Tuberkulosis Paru Pada Rumah Sakit Panti Waluyo Purworejo. *Journal of International Multidisciplinary Research*, *2*(3), 1–11.

Enda, M., & Rukiyanto, B. A. (2024). Kontribusi Penghayatan Spiritualitas Prodiakon Paroki Kristus Raja Baciro Bagi Pelayanan. *Divinitas Jurnal Filsafat Dan Teologi Kontekstual*, *2*(1), 1–20.

Faiz, M. N., Somantri, O., Supriyono, A. R., & Muhammad, A. W. (2022). Impact of feature selection methods on machine learning-based for detecting DDoS attacks: Literature review. *Journal of Informatics and Telecommunication Engineering*, *5*(2), 305–314.

Fauzi, A. M. (2024). *KLASIFIKASI SERANGAN MALWARE ANDROID BERDASARKAN ANALISIS FITUR DINAMIS MENGGUNAKAN ALGORITMA RANDOM FOREST*. Universitas Siliwangi.

Febriani, S., Bahri, S., & Dewantara, R. (2024). ANALISIS PERANCANGAN SISTEM PENERIMAAN SANTRI BERPRESTASI MENGGUNAKAN KOMBINASI METODE

AHP-WP: ANALISIS PERANCANGAN SISTEM PENERIMAAN SANTRI BERPRESTASI MENGGUNAKAN KOMBINASI METODE AHP-WP. *Informasi Interaktif: Jurnal Informatika Dan Teknologi Informasi*, *9*(1).

Firdaus, R., Hadiana, A. I., & Kasyidi, F. (2022). Model Deteksi Botnet Menggunakan Algoritma Decision Tree Dengan Untuk Mengidentifikasi Serangan Click Fraud. *Journal of Informatics and Communication Technology (JICT)*, *4*(2), 10–20.

Khairulah, R. A., Herdianto, R., & Setiawan, M. A. (2023). Klasifikasi Serangan Pada Jaringan Internet of Thing (IoT): Tinjauan Literatur Komparatif. *Jurnal Inovasi Teknologi Dan Edukasi Teknik*, *3*(1), 47–53.

Kuntjoro, Y. D. (2023). Analisis Perilaku Entitas untuk Pendeteksian Serangan Internal Menggunakan Kombinasi Model Prediksi Memori dan Metode PCA. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(6), 1223–1232.

Matin, I. M. M., Agustin, M., Sugiarto, B., & Asri, A. N. (2023). DETEKSI MALWARE MENGGUNAKAN MACHINE LEARNING DENGAN METODE ENSEMBLE. *Prosiding Seminar Sains Nasional Dan Teknologi*, *13*(1), 265–270.

Mayasari, N., Dewantara, R., & Yuanti, Y. (2023). Pengaruh kecerdasan buatan dan teknologi pendidikan terhadap peningkatan efektivitas proses pembelajaran mahasiswa di jawa timur. *Jurnal Pendidikan West Science*, *1*(12), 851–858.

Mindara, C. L., Zulianto, A., Utomo, H. P., Hatati, T., & Sudrajat, D. (2023). Convolutional Neural Network Deteksi Intrusi Untuk Klasifikasi Serangan Jaringan Dengan Penerapan Algoritma Convolutional Neural Network. *Jurnal ICT: Information Communication & Technology*, *23*(2), 517–522.

Munawar, Z., & Putri, N. I. (2020). Keamanan IoT Dengan Deep Learning dan Teknologi Big Data. *TEMATIK*, *7*(2), 161–185.

Nainggolan, H., & Dewantara, R. (2023). DAMPAK PROMOSI ONLINE SERTA MUTU LAYANAN PENGIRIMAN KEPADA LOYALITAS KONSUMEN TERHADAP APLIKASI GRAB. *Journal of Computer Science and Information Technology*, *1*(1), 44–58.

Pranata, E. J., & Dewantara, R. (n.d.). Analisis Dan Pengukuran Quality Of Service (Qos) Jaringan 4G (Operator Telkomsel, Xl, Dan Indosat). *Cyber Security Dan Forensik Digital*, *6*(2), 69–75.

Putra, C. A., Pratama, R., & Sutabri, T. (2023). ANALISIS MANFAAT MACHINE LEARNING PADA NEXT-GENERATION FIREWALL SOPHOS XG 330 DALAM MENGATASI SERANGAN SQL INJECTION. *Jurnal Manajemen Informatika Dan Sistem Informasi*, *6*(2), 197–204.

Rafrastara, F. A., Supriyanto, C., Paramita, C., & Astuti, Y. P. (2023). Deteksi Malware menggunakan Metode Stacking berbasis Ensemble. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(1), 11–16.

Ramadhan, A., Lindawati, L., & Rose, M. M. (2023). Komparasi Algoritma Neural Network dan K-Nearest Neighbor Dalam Mendeteksi Malware Android. *Building of Informatics, Technology and Science (BITS)*, *5*(1), 191–199.

Ramdan, A. (2021). *ANALISA ANCAMAN SERANGAN MALWARE PADA TRAFIK DARKNET MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBOUR*. Universitas Siliwangi.

Ramdan, A., Siliwangi, U., Widyasono, N., Siliwangi, U., Mubarok, H., & Siliwangi, U. (2022). Prediksi Jaringan TOR dan VPN menggunakan Algoritma K-Nearest Neighbour pada Trafik Darknet. *Vol*, *5*, 21–35.

Rukiyanto, B. A., Christiani, T. K., & Almirzanah, S. (2024). Religious education to develop respect for plurality in Indonesia. *Journal of Beliefs & Values*, 1–16.

Sandriana, A., & Maulana, F. (2022). Klasifikasi serangan malware terhadap lalu lintas jaringan Internet of Things menggunakan Algoritma K-Nearest Neighbour (K-NN). *E-JOINT (Electronica and Electrical Journal Of Innovation Technology)*, *3*(1), 12–22.

Sari, L. P. (2022). Pendidikan Kesehatan Tentang Pentingnya Personal Hygiene Pada Masa Nifas di Puskesmas Bowong Cindea Kab. Pangkep. *Jurnal Altifani Penelitian Dan Pengabdian Kepada Masyarakat*, *2*(2), 161–168.

Sugiyono. (2018). *Metodelogi Penelitian Kuantitatif, Kualitatif, dan R&G*. ALFABETA.

Syarif, A. K. (2021). *Sistem Klasifikasi Penyakit Tanaman Cabai Menggunakan Metode Deep Learning dengan Library TensorFlow Lite*. Universitas Hasanuddin.

Tjahjadi, E. V. (2023). Klasifikasi Malware Menggunakan Teknik Machine Learning. *Jurnal Ilmiah Ilmu Komputer Banthayo Lo Komputer*, *2*(1), 60–70.

Tundo, T., & Dewantara, R. (2024). Penentuan Penerima BSM untuk Menghindari Subyektivitas Penerima Berdasarkan Metode Decision Support System VIKOR. *Prosiding TAU SNARS-TEK Seminar Nasional Rekayasa Dan Teknologi*, *3*(1), 241–250.

Wahid, M. I., Mustamin, S. A., & Lawi, A. (2021). Identifikasi Dan Klasifikasi Citra Penyakit Daun Tomat Menggunakan Arsitektur Inception V4. *Proceeding KONIK (Konferensi Nasional Ilmu Komputer)*, *5*, 257–264.

Widyasono, N., & Mubarok, H. (2022). Darknet, Malware, KNN, Forensik Prediksi Jaringan TOR dan VPN menggunakan Algoritma K-Nearest Neighbour pada Trafik Darknet. *Jurnal Sistem Cerdas*, *5*(1), 21–35.